UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/516,966	07/29/2005	Jean-Claude Pailles	18394-009US1	3136

26221 7590 06/19/2009

FISH & RICHARDSON P.C.
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
06/19/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

Office Action Summary	Application No.	Applicant(s)	
	10/516,966	PAILLES ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 March 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13 and 15-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13 and 15-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

FINAL ACTION

1. This action is in response to amendment filed 3/24/2009. Claims 1-13 and 15-25 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-13 and 15-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishiguro et al. (European Patent Application EP 0856821 and hereinafter Ishiguro (Reference cited from IDS)) in view of Barlow et al. (US Patent No. 2004/0215964 and Barlow hereinafter), further in view of Deindl et al (US Patent No. 6,076,162 and Deindl hereinafter).

3. As to claim 1, Ishiguro teaches a method for checking a digital signature, involving a microcircuit connectable to a data processing system, the microcircuit (e.g. IC card) being designed to receive requests to check digital signatures from the data processing system [col. 7, lines 35-40], and to process these requests, a digital signature being generated using a private key (i.e., secret key pT and qT) only known to

a signatory entity (i.e., Terminal) and associated with a public key (i.e., Terminal public key nT) [col. 5, lines 10-25], and a phase of checking (i.e., verifying) a digital signature [col. 20, lines 25-27] comprising steps of:

receiving by the microcircuit (e.g. IC card) a digital signature to be checked and a public key in a pair of keys comprising a private key that was used to generate the digital signature to be checked (i.e., verify) [col. 9, lines 30-35].

Ishiguro does not teach: involving a microcircuit connectable to a data processing system. However, these features are well known in the art and would have been an obvious modification of the system disclosed by Ishiguro as introduced by Barlow. Barlow discloses: involving a microcircuit connectable to a data processing system (to provide verification of a microcircuit connected to a data processing system [fig. 1] .

Therefore, given the teachings of Barlow, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Ishiguro by employing the well known features of chipcard verification in a data processing environment disclosed above by Barlow, for which security in a data processing environment authentication will be enhanced [Figure 1].

Ishiguro in view of Barlow does not teach: said method comprising a step of storing a certificates table containing a digest form of at least one public key in a memory in the microcircuit, calculating a digest form of the received public key, and decrypting the

digital signature using the received public key if the calculated digest form of the public key is located in the certificates table, and searching for the calculated digest form of the public key in the certificates table.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Ishiguro in view of Barlow as introduced by Deindl. Deindl discloses:

said method comprising a step of storing a certificates table containing a digest form of at least one public key (i.e., certificate key) in a memory in the microcircuit (to store a public key digest in a chipcard [col. 2, lines 45-55]), calculating a digest form (i.e., hash) of the received public key (i.e., first part) (to create a fingerprint of a key [col. 5, lines 5-10]), and decrypting the digital signature using the received public key if the calculated digest form of the public key is located in the certificates table (to verify if the certificate key can be used [col. 6, lines 15-20]) and searching for the calculated digest form of the public key in the certificates table (e.g., stored on the chipcard) (to perform a certificate key search [col. 5, lines 60- 67]).

Therefore, given the teachings of Deindl, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Ishiguro in view of Barlow by employing the well known features of certification of cryptographic keys for chip cards disclosed above by Deindl, for which chipcard signature authentication will be enhanced [col. 6, lines 15-20].

4. As to claim 2, Ishiguro teaches a method further comprising a phase of inserting a public key into the certificates table, comprising steps consisting of: receiving by the microcircuit a certificate of the public key to be inserted in the certificates table (i.e., Ishiguro teaches pre-storing a master public key on IC Card [col. 29, lines 25-27]), and a public key from a certification entity that generated the certificate [col. 29, lines 25-27], the certificate comprising the public key to be added (i.e., pre-storing) into the certificates table (i.e. predetermine area, EEPROM) and a digital signature (i.e., master digital signature) of the certification entity [col. 29, lines 20- 25], generated using a private key belonging to a pair of keys including the public key of the certification entity. Ishiguro does not teach:

calculating by the microcircuit a digest form of the public key received from the certification entity decrypting the digital signature using the public key received from the certification entity if the calculated digest form of the public key is located in the table extracting the public key to be inserted from the certificate if the decrypted digital signature is correct, calculating a digest of the public key extracted from the certificate, and inserting the calculated digest in the certificates table (i.e., public key pre-stored/col. 29, lines 10-25), and searching for the calculated digest form of the public key in the certificates table.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Ishiguro as introduced by Deindl. Deindl discloses:

calculating a digest form of the public key received from the certification entity (to calculate a hash of a cryptographic key [col. 6, lines 15-21]) decrypting the digital signature using the public key received from the certification entity if the calculated digest form of the public key is located in the table (to perform a cryptographic function on the digital signature using a certification key [col. 6, lines 5- 15]) extracting the public key to be inserted from the certificate if the decrypted digital signature is correct (to provide mean to verify cryptographic key [fig. 1]),

inserting (i.e., storing) the calculated digest (i.e., first part) in the certificates table (to provide means to store the hash in the chipcard [col. 5, lines 50-55]), and searching for the calculated digest form of the public key in the certificates table (e.g., stored on the chipcard) (to perform a certificate key search [col. 5, lines 60- 67]).

Therefore, given the teachings of Deindl, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Ishiguro by employing the well known features of certification of cryptographic keys for chip cards disclosed above by Deindl, for which chipcard signature authentication will be enhanced [col. 6, lines 15-20].

5. As to claims 3 and 4, the system disclose by Ishiguro teaches substantial features of the claim invention (discussed above) but it fails to disclose:

A method where the phase of inserting a public key in the certificates table comprises a step of inserting in the certificates table of a pointer to the digest of the public key of the certification entity that issued the certificate of the public key to be inserted, so as to define a certification tree in combination with the inserted digest of the public key (claim 3).

A method further comprising a phase of deleting a digest of a public key from the certificates table, comprising steps of deleting from the certificates table the digest of a public key to be removed, and deleting from the certificates table all digests of public keys associated with a pointer indicating the public key to be removed (claim 4).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Ishiguro as introduced by Barlow. Barlow discloses:

A method where the phase of inserting a public key in the certificates table comprises a step of inserting in the certificates table of a pointer to the digest of the public key of the certification entity that issued the certificate of the public key to be inserted, so as to define a certification tree in combination with the inserted digest of the public key (claim 3) (to provide certificate inserting capability to a IC Card [par. 45]).

A method further comprising a phase of deleting a digest of a public key from the certificates table, comprising steps of deleting from the certificates table the digest of a

public key to be removed, and deleting from the certificates table all digests of public keys associated with a pointer indicating the public key to be removed (claim 4) (to provide certificate deleting capability from a IC Card [par. 45]).

Therefore, given the teachings of Barlow, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Ishiguro by employing the well known features of inserting and deleting certificate disclosed above by Barlow, for which IC Card signature authentication will be enhanced [par. 45].

6. As to claim 5, Ishiguro teaches a method where each public key digest entered into the certificates table is associated with a validity end date (i.e., term of validity [col. 29, lines 10-20]), the phase of inserting a public key into the certificates table further comprising steps of reading in a received certificate (i.e., public key) a validity end date (i.e., term of validity [col. 29, lines 10-20]) of the public key to be inserted (i.e., public key pre-stored), and entering the validity end date (i.e., term of validity) of the public key to be inserted into the certificates table (i.e., tem of validity stored on the IC Card [col. 29, lines 10-20]), together with the digest of the public key to be inserted (i.e., pre-stored public key), if it is earlier than the validity end date of the public key of the certification entity read in the certificates table (i.e., Ishiguro teaches verifying the validity of signature containing the public key. Ishiguro teaches if valid performing read operation [col. 7, lines 35-45]).

7. As to claim 6, Ishiguro teaches a method where each digest of a public key entered in the certificates table is associated with a usage counter (i.e., term of validity) that is incremented every time that a digital signature is checked using the public key [i.e., use of public key/col. 31, lines 1-10] (i.e., Ishiguro teaches storing term of validity information [col. 29, lines 15-20]. Ishiguro teaches a value for which a usage determination is made base on said value [col. 31, lines 5-20] Ishiguro teaches subtracting from available value subsequent of usage).

However Ishiguro does not expressly teach: said method comprising deletion of a public key digest from the certificates table when the usage counter is zero and the number of empty locations in the certificates table is less than a predetermined threshold.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Ishiguro as introduced by Barlow. Barlow discloses:

said method comprising deletion of a public key digest from the certificates table when the usage counter is zero and the number of empty locations in the certificates table is less than a predetermined threshold (to provide certificate deleting capability from a IC Card [par. 45]).

Therefore, given the teachings of Barlow, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Ishiguro by employing the well known features of deleting a certificate as disclosed above by Barlow, for which IC Card signature authentication will be enhanced [par. 45].

8. As to claim 7, Ishiguro teaches a method where each public key digest entered into the certificates table is associated with a usage counter that is incremented every time that a digital signature is checked using the public key [col. 31, lines 35-45], and with a last usage date that is updated every time that the associated usage counter is incremented [col. 31, lines 35-45] ((i.e., Ishiguro teaches storing term of validity information [col. 29, lines 15-20]. Ishiguro teaches a value for which a usage determination is made base on said value [col. 31, lines 5-20]. Ishiguro teaches subtracting from available value subsequent of usage).

However Ishiguro does not expressly teach: said method further comprising a step to select a digest of a public key to be deleted as a function of the corresponding associated values of the usage counter and the last usage date when the number of empty locations in the certificates table is less than a predetermined threshold.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Ishiguro as introduced by Barlow. Barlow discloses:

said method further comprising a step to select a digest of a public key to be deleted as a function of the corresponding associated values of the usage counter and the last usage date when the number of empty locations in the certificates table is less than a predetermined threshold (to provide IC Card information management of secure storage [par. 56 - par. 57]).

Therefore, given the teachings of Barlow, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Ishiguro by employing the well known features of IC Card information management of secure storage disclosed above by Barlow, for which IC Card signature authentication will be enhanced [par. 56 - par. 57].

9. As to claim 8, the system disclose by Ishiguro teaches substantial features of the claim invention (discussed above) it fails to disclose:

A method where the microcircuit uses a predefined hashing function to calculate the digest forms of the public keys.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Ishiguro as introduced by Deindl. Deindl discloses:

A method where the microcircuit uses a predefined hashing function to calculate the digest forms of the public keys (to calculate the hash of a cryptographic key [col. 6, lines 15-20]).

Therefore, given the teachings of Deindl, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Ishiguro by employing the well known features of calculating a hash for a cryptographic key disclosed above by Deindl, for which chipcard signature authentication will be enhanced [col. 6, lines 15-20].

10. As to claim 9, Ishiguro teaches a method further comprising a phase of inserting a root (i.e., master) public key in the certificates table (i.e., Ishiguro teaches pre-storing a master public key on IC card [col. 29, lines 20-30]), this insertion phase being done by a write processing controlled by a MAC calculated using a specific key in the microcircuit and only known to an entity having issued the microcircuit (i.e., Ishiguro teaches a card dispenser which records initial information on to the IC card [col. 29, lines 20-25]).

11. As to claim 10, Ishiguro teaches a method where the digest of a public key memorized in the certificates table is obtained by calculating a digest of the public key associated with other information such as the validity end date of the public key (i.e., Ishiguro teaches the utilization of a computation method involving receiving a signature

and key for a sender. Inputting the signature and key into a signature verification function. The computed results are compared with a predetermined condition for verification purposes [col. 2, lines 45-58]).

However Ishiguro does not expressly teach: identity information and serial numbers, this information being transmitted to the microcircuit every time that the signature is checked using the public key.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Ishiguro as introduced by Barlow. Barlow discloses: identity information and serial numbers, this information being transmitted to the microcircuit every time that the signature is checked using the public key (to provide certificate transmittal capability [par. 84]).

Therefore, given the teachings of Barlow, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Ishiguro by employing the well known features of certificate transmittal disclosed above by Barlow, for which IC Card signature authentication will be enhanced [par. 84].

12. As to claim 11, the system disclose by Ishiguro teaches substantial features of the claim invention (discussed above) but it fails to disclose a method where the digest of a public key memorized in the certificates table is obtained by calculating a digest of

the certificate received by the microcircuit when the public key is inserted in the certificates table, this certificate being transmitted to the microcircuit every time that the signature is checked using the public key.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Ishiguro as introduced by Deindl. Deindl discloses:

A method where the digest of a public key memorized in the certificates table is obtained by calculating a digest (i.e., fingerprint) of the certificate (i.e., first part) received by the microcircuit when the public key is inserted in the certificates table (to calculate the digest of the received certificate [col. 5, lines 15-21]), this certificate being transmitted to the microcircuit every time that the signature is checked using the public key (to provide for transferring a certificate for signature verification [fig. 1]).

Therefore, given the teachings of Deindl, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Ishiguro by employing the well known features of calculating a hash of cryptographic key disclosed above by Deindl, for which chipcard signature authentication will be enhanced [fig. 1].

13. As to claim 12, the system disclose by Ishiguro teaches substantial features of the claim invention (discussed above) it fails to disclose:

A method where the certificates table is stored in a secure memory area in the microcircuit.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Ishiguro as introduced by Deindl. Deindl discloses:

A method where the certificates table (i.e., certification key) is stored (i.e., transferred) in a secure memory area in the microcircuit (to provide for storing certificate keys [col. 6, lines 40-50]).

Therefore, given the teachings of Deindl, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Ishiguro by employing the well known features of certification of cryptographic keys for chip cards disclosed above by Deindl, for which chipcard signature authentication will be enhanced [col. 6, lines 15-20].

14. As to claim 13, Ishiguro teaches a microcircuit, designed to receive requests to check digital signatures from a data processing system, and to process these requests, a digital signature being generated using a private key only known to a signatory entity and associated with a public key, said microcircuit comprising:

means for receiving a digital signature to be checked and a public key in a pair of keys comprising a private key that was used to generate the digital signature to be checked [col. 7, lines 35-40].

However Ishiguro does not expressly teach: means for calculating a digest form of the received public key, and means for decrypting the digital signature using the received public key, memory means for storing a certificates table containing a digest form of at least one public key, and for searching for the calculated digest form of the public key in the certificates table.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Ishiguro as introduced by Dendl. Dendl discloses:

means for calculating a digest form of the received public key (to calculate the hash of a cryptographic key [col. 6, lines 15-20]), and means for decrypting (i.e., converted) the digital signature using the received public key (to provide a cryptographic function using the received certification key [col. 6, lines 5-10]) memory means for storing a certificates table containing a digest form of at least one public key (to provide for storing certificate keys [col. 6, lines 40-50]) and searching for the calculated digest form of the public key in the certificates table (e.g., stored on the chipcard) (to perform a certificate key search [col. 5, lines 60- 67]).

Therefore, given the teachings of Dendl, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Ishiguro by employing the well known features of the certification of cryptographic key for chipcard disclosed above by Dendl, for which IC Card signature authentication will be enhanced [col. 6, lines 5-10].

15. 14 (canceled)

16. As to claim 15, Ishiguro teaches a microcircuit further comprising: means for receiving a certificate of the public key to be inserted in the certificates table (i.e., Ishiguro teaches a card dispenser records a initial information to the IC Card [col. 29, lines 20-25]), and a public key from a certification entity that generated the certificate, the certificate comprising the public key to be added (i.e., pre-stored on IC Card) into the certificates table and a digital signature of the certification entity (i.e., Ishiguro teaches a master public key and digital signature pre- stored on IC Card [col. 29, lines 20-20]), generated using a private key belonging to a pair of keys including the public key of the certification entity.

However Ishiguro does not expressly teach: means for calculating a digest form of the public key received from the certification entity, means for decrypting the digital signature using the public key received from the certification entity if the calculated digest form of the public key is located in the table, means for extracting the public key

to be inserted from the certificate if the decrypted digital signature is correct, means for calculating a digest of the public key extracted from the certificate, and for inserting the calculated digest in the certificates table, and for searching for the calculated digest form of the public key in the certificates table.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Ishiguro as introduced by Deindl. Deindl discloses:

means for calculating a digest form of the public key received from the certification entity (to calculate a hash of a cryptographic key [col. 6, lines 15-21]) means for decrypting the digital signature using the public key received from the certification entity if the calculated digest form of the public key is located in the table (to perform a cryptographic function on the digital signature using a certification key [col. 6, lines 5-15]) means for extracting the public key to be inserted from the certificate if the decrypted digital signature is correct (to provide mean to verify cryptographic key [fig. 1D, means for calculating a digest of the public key extracted from the certificate (to calculate the hash of a cryptographic key (col. 6, lines 15-21), and for inserting (i.e., storing) the calculated digest (i.e., first part) in the certificates table (to provide means to store the hash in the chipcard [col. 5, lines 50- 55]), and searching for the calculated digest form of the public key in the certificates table (e.g., stored on the chipcard) (to perform a certificate key search [col. 5, lines 60- 67]).

Therefore, given the teachings of Deindl, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Ishiguro by employing the well known features of certification of cryptographic key for chipcards disclosed above by Deindl, for which signature authentication will be enhanced [col. 5, lines 60-67].

17. As to claims 16 and 17, the system disclose by Ishiguro teaches substantial features of the claim invention (discussed above) it fails to disclose:

A microcircuit further comprising means for inserting in the certificates table a pointer to the digest of the public key of the certification entity that issued the certificate of the public key to be inserted, so as to define a certification tree in combination with the inserted digest of the public key (claim 16).

A microcircuit further comprising means for deleting from the certificates table a digest of a public key to be removed, and means for deleting from the certificates table all digests of public keys associated with a pointer indicating the public key to be removed (claim 17).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Ishiguro as introduced by Barlow. Barlow discloses:

A microcircuit further comprising means for inserting in the certificates table a pointer to the digest of the public key of the certification entity that issued the certificate

of the public key to be inserted, so as to define a certification tree in combination with the inserted digest of the public key (claim 16) (to provide certificate inserting capability to a IC Card [par. 45]).

A microcircuit further comprising means for deleting from the certificates table a digest of a public key to be removed, and means for deleting from the certificates table all digests of public keys associated with a pointer indicating the public key to be removed (claim 17) (to provide certificate deleting capability from a IC Card [par. 45]).

Therefore, given the teachings of Barlow, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Ishiguro by employing the well known features of inserting and deleting certificate disclosed above by Barlow, for which IC Card signature authentication will be enhanced [par. 45].

18. As to claim 18, Ishiguro teaches a microcircuit further comprising: means for reading in a received certificate a validity end date of a public key to be inserted [col. 29, lines 20-25], and means for entering the validity end date of the public key to be inserted into the certificates table (i.e., tem of validity stored on the IC Card [col. 29, lines 10-20]), together with the digest of the public key to be inserted [col. 29, lines 20-30], if the validity end date is earlier than the validity end date of the public key of the certification entity read in the certificates table (i.e., Ishiguro teaches verifying the

validity of signature containing the public key. Ishiguro teaches if valid performing read operation [col. 7, lines 35-45]).

19. As to claim 19, Ishiguro teaches a microcircuit further comprising means for incrementing a usage counter associated with each public key digest entered into the certificates table, every time that a digital signature is checked using the public key (i.e., Ishiguro teaches storing term of validity information [col. 29, lines 15-20]. Ishiguro teaches a value for which a usage determination is made base on said value [col. 31, lines 5-20]. Ishiguro teaches subtracting from available value subsequent of usage).

However Ishiguro does not expressly teach: means for deleting a public key digest from the certificates table when the associated usage counter is zero and the number of empty locations in the certificates table is less than a predetermined threshold.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Ishiguro as introduced by Barlow. Barlow discloses: means for deleting a public key digest from the certificates table when the associated usage counter is zero and the number of empty locations in the certificates table is less than a predetermined threshold (to provide certificate deleting capability from a IC Card [par. 45]).

Therefore, given the teachings of Barlow, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Ishiguro by employing the well known features of deleting certificate disclosed above by Barlow, for which IC Card signature authentication will be enhanced [par. 45].

20. As to claim 20, Ishiguro teaches a microcircuit further comprising means for updating a last usage date associated with each public key digest entered into the certificates table, every time that a digital signature is checked using the public key (i.e., Ishiguro teaches storing term of validity information [col. 29, lines 15-20]. Ishiguro teaches a value for which a usage determination is made base on said value [col. 31, lines 5-20]. Ishiguro teaches subtracting from available value subsequent of usage), However Ishiguro does not expressly teach:

means for deleting a public key digest from the certificates table when the number of empty locations in the certificates table is less than a predetermined threshold, and means for selecting a digest of a public key to be deleted as a function of the corresponding associated values of the usage counter and the last usage date.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Ishiguro as introduced by Barlow. Barlow discloses:

means for deleting a public key digest from the certificates table when the number of empty locations in the certificates table is less than a predetermined

threshold (to provide certificate deleting capability from a IC Card [par. 45]), and means for selecting a digest of a public key to be deleted as a function of the corresponding associated values of the usage counter and the last usage date (to provide IC Card information management of secure storage [par. 56 - par. 57]).

Therefore, given the teachings of Barlow, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Ishiguro by employing the well known features of IC Card information management disclosed above by Barlow, for which IC Card signature authentication will be enhanced [par. 56- par. 57]).

21. As to claim 21, the system disclose by Ishiguro teaches substantial features of the claim invention (discussed above) it fails to disclose:

A microcircuit further comprising means for executing a predefined hashing function to calculate the digest forms of the public keys. However, these features are well known in the art and would have been an obvious modification of the system disclosed by Ishiguro as introduced by Deindl. Deindl discloses:

A microcircuit further comprising means for executing a predefined hashing function to calculate the digest forms of the public keys (to calculate the hash of a cryptographic key [col. 6, lines 15-20]).

Therefore, given the teachings of Deindl, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Ishiguro by employing the well known features of calculating a hash for a cryptographic key disclosed above by Deindl, for which chipcard signature authentication will be enhanced [col. 6, lines 15-20].

22. As to claim 22, Ishiguro teaches a method further comprising means for inserting a root (i.e., master) public key in the certificates table (i.e., Ishiguro teaches pre-storing a master public key on IC card [col. 29, lines 20-30]), using a write processing controlled by a MAC calculated using a specific key in the microcircuit and only known to an entity having issued the microcircuit (i.e., Ishiguro teaches a card dispenser which records initial information on to the IC card [col. 29, lines 20-25]).

23. As to claim 23, Ishiguro teaches a method where the means for calculating the digest of a public key memorized in the certificates table comprise means for calculating a digest of the public key associated with other information comprising the validity end date (i.e., term of validity) of the public key, identity information and serial numbers (i.e., identification number), this information being transmitted to the microcircuit (i.e., IC terminal) every time that the signature is checked (i.e., signature checked by IC terminal) using the public key [claim 1, col. 30, lines 25-45].

24. As to claims 24 and 25, the system disclose by Ishiguro teaches substantial features of the claim invention (discussed above). It fails to disclose:

A method where the means for calculating the digest of a public key memorized in the certificates table comprise means for calculating a digest of the certificate received by the microcircuit when the public key is inserted in the certificates table, this certificate being transmitted to the microcircuit every time that the signature is checked using the public key (claim 24).

A method according where the memory means for storing the certificates table is a secure memory area (claim 25).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Ishiguro as introduced by Le. Le discloses:

A method where the means for calculating the digest of a public key memorized in the certificates table comprise means for calculating a digest of the certificate received by the microcircuit when the public key is inserted in the certificates table (to calculate cryptographic key hash [col. 6, lines 5-20]), this certificate being transmitted to the microcircuit every time that the signature is checked using the public key (claim 24) (to transmit a certificate to chipcard [fig. 1]).

A method according where the memory means for storing the certificates table is a secure memory area (claim 25) (to provide for storing certificate keys [col. 6, lines 40-50]).

Therefore, given the teachings of Deindl, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Ishiguro by employing the well known features of calculating a hash for a cryptographic key and key storage disclosed above by Deindl, for which chipcard signature authentication will be enhanced [col. 6, lines 15-20].

Response to Arguments

Applicant's arguments filed 3/24/2009 have been fully considered but they are not persuasive. Applicant alleges the combination of Ishiguro, Barlow, and Deindl is deficient in teaching claim limitation elements, "storing a certificate table containing a digest form of at least one public key" and "searching for the calculated digest form of the public key in the certificate table".

Examiner contends those skill in the art would recognize applicant's usage of the term "table" as well known in the art as a data structure. Such a data structure the Examiner respectfully submits is an allocation of memory (e.g., list, table, array, vector). Thus, the teaching of Ishiguro, col. 15, lines 30-40 teaches, "in their card (e.g., smart card) information area (e.g., memory) are configured to have (e.g., stored) public key". In addition to the Ishiguro teachings, the Examiner respectfully submits the teachings of

Barlow, paragraph 37 teaches "the IC card stores public and private key pairs and related public key certificate". Moreover, the Examiner contends the teachings of Deindl, column 6, lines 43-46 recites a memory location in a chip card containing a list (e.g., table) of keys. The teachings of Deindl further recites hashing the information stored on the chip card to compress the data in column 49-54.

With regards to applicant's claim element of "searching for the calculated digest form of the public key in the certificate table, the Examiner respectfully submits, that Deindl teaches, "searching for the certification key in the card" column 5, lines 60-65. Recall the previous citing of Deindl teachings for which recited a memory location in the chip card containing a list (tables) of keys. Therefore, based on the teachings of the prior art, Examiner contends applicant's arguments are non-persuasive. Examiner maintains the 35 USC 103 rejection under the combination of Ishiguro, Barlow, and Deindl.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431